chainfrog

Leonidas After-Work 11.1.2017

HELLO WORLD!

Kimmo Rouhiainen
Business Advisor, 1000+ business cases
+358 40 583 1100
kimmo@chainfrog.com

Keir Finlow-Bates
CEO, 16 patents, mathematican
+358 44 0101 893
keir@chainfrog.com

www.chainfrog.com

chainfrog

WHO ARE WE?

- Finnish blockchain software company
- Offering consultancy, workshops, project collaboration, product development
- 5 patents pending
- Demo software at https://wherecoin.com:555
- We know blockchains

Find us at www.chainfrog.com

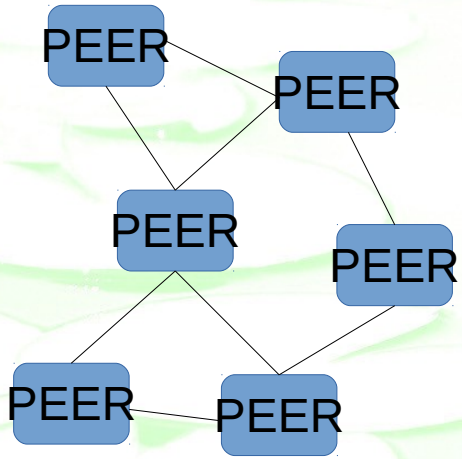
What is a Blockchain?

Simple answer:
AN EXTENSION TO A DATABASE

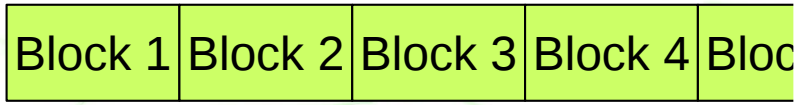
What is a Blockchain?

More complicated answer:

1: A peer-to-peer network



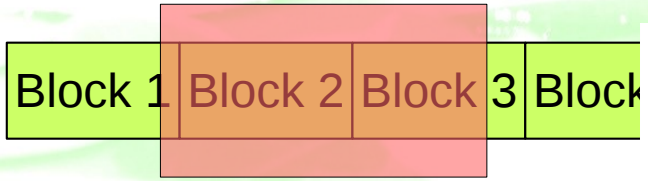
2: A blockchain file



3: A consensus protocol

```
sha256(sha256(block)) < difficulty
```

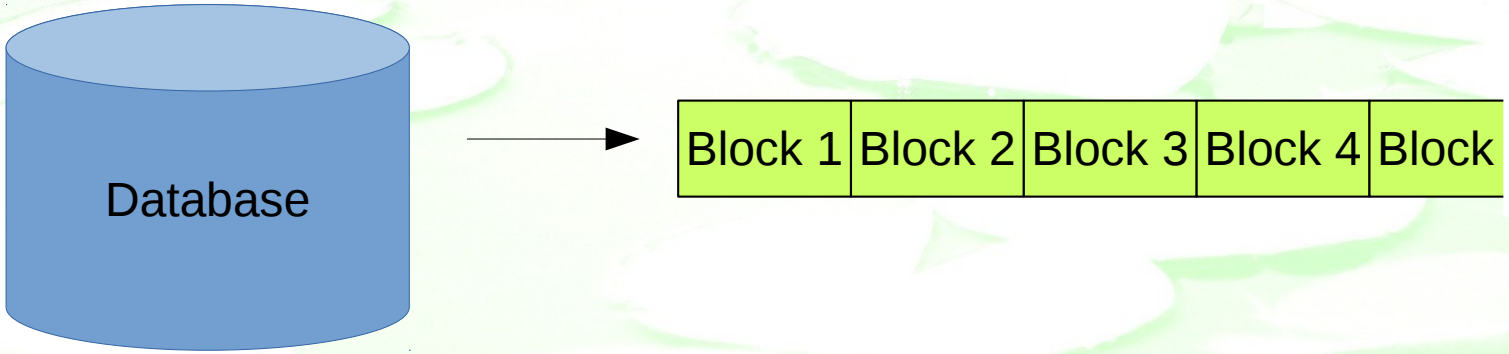
4: A blockchain parser



What is a Blockchain?

It’s stored in a file?

- In practice the details of the blockchain are stored in a database
- Usually there is the option to “dump” the chain to a file, e.g. for quick transferal to another node



- For practical purposes the blockchain is stored in a database so we can use over 50 years of innovation to search and extend it

History Lesson

1960s: IBM introduces hierarchical databases (moonshot).

1970: Edgar Frank Codd, working at IBM, publishes the Relational Database Model. IBM sticks with the hierarchical model (RDBM too slow...).

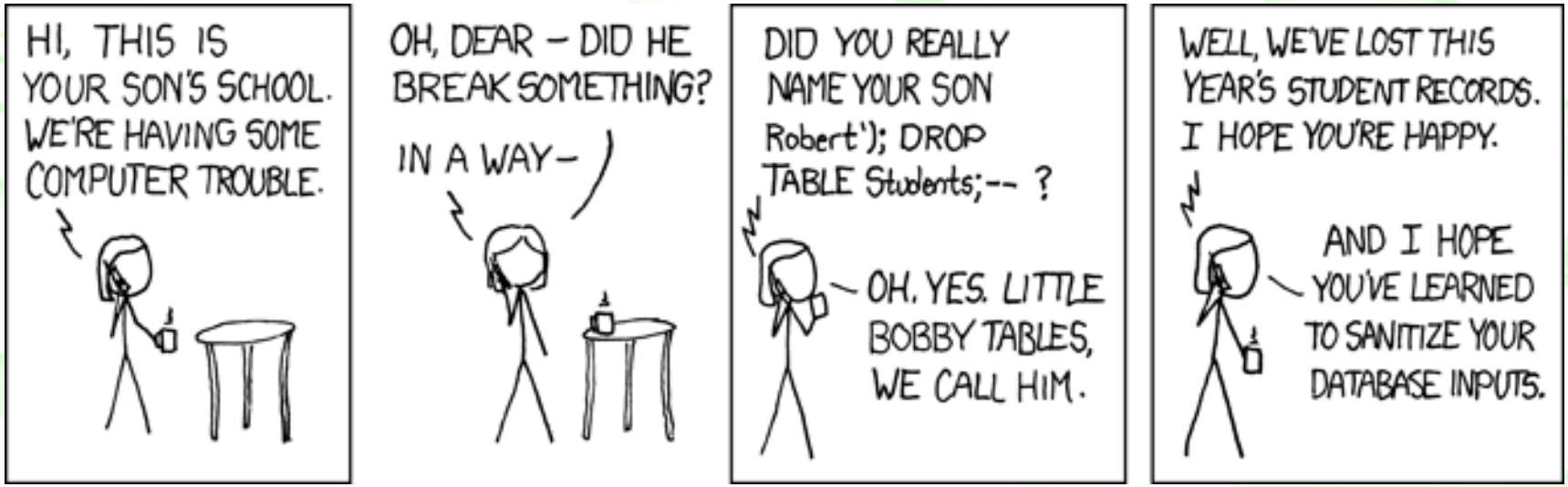
1979: Oracle releases the first commercial RDMS. SQL starts to become popular. Oracle becomes rich.

2008: Nakamoto publishes “Bitcoin: A Peer-to-Peer Electronic Cash System”

2016: Most databases are RDMS. Oracle, MySQL, Microsoft SQL Server, PostgreSQL and IBM DB2 are the most popular implementations. NoSQL and distributed databases are gaining popularity for big data purposes

Traditional Database Weaknesses

- Records can be altered without a trace if incorrectly configured, or by a skilled administrator.
- Centralized by design, relying on client/server model.
- Problems with backups, synchronization across multiple database centers, concurrent record editing, and so on.



(Credit: http://xkcd.com)

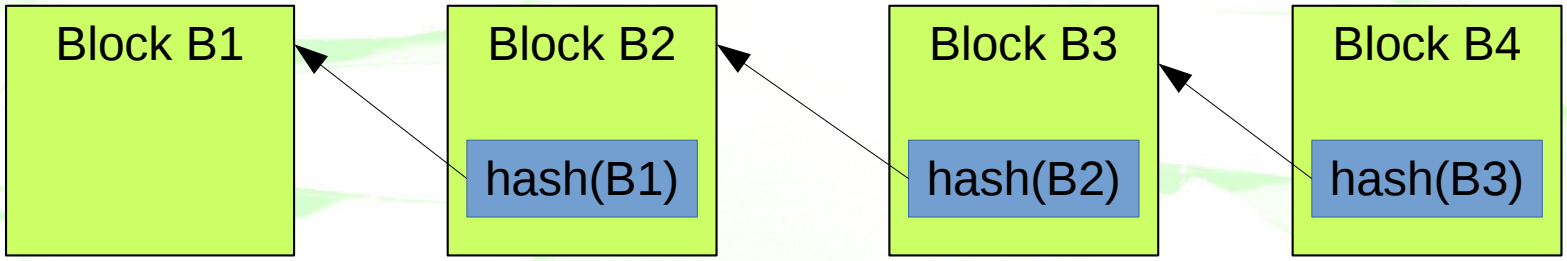
See also: people with the surname Null

What is a Blockchain?

- A method of storing data in a sequential chain of blocks.
- Each block is a package of data created within a short consecutive window of time.
- A block has its own “hash”, based on the data it contains, which is like a fingerprint that uniquely identifies it.
- As time progresses, it gets computationally harder to alter the earlier blocks (they become tamper-proof)
- The blockchain participants use a consensus protocol to decide which data gets added next

What is a Blockchain?

- Each block (except the first “genesis block”) contains a reference to the block before it using the previous block’s hash, thereby forming a chain.



- The earlier blocks in the chain cannot be tampered with, because changing a block changes its hash, and this would break the chain of references.

How are Blocks Added to a Blockchain?

- Some of the devices on a peer-to-peer network regularly transmit data onto the network, to be included in the next block (the clients).
- Other devices (nodes, validators or miners) receive and package the data into their own proposed block and then hold a lottery (consensus system) to see which device was lucky enough to create the block to be included.
- They do this because there is a reward for creating the next new block (public blockchains), or because they are run by entities who value the availability of the blockchain (private blockchains).

How are Blocks Added to a Blockchain?

- The lottery odds are adjusted occasionally to ensure that new blocks are accepted at roughly the same regular interval, for example every ten minutes or so.

- There are a number of consensus protocols:

  - “proof-of-work” (used by Bitcoin, Ethereum)
  - “proof-of-stake” (proposed for Ethereum)
  - “practical Byzantine fault tolerance” (Hyperledger Fabric)
  - “proof of elapsed time” (Hyperledger Sawtooth Lake)
  - “round robin” (Multichain)
  - “multisig” (bigchainDB, Corda)

Types of Blockchain

Type	Description	Example Use
Public	The blockchain is available freely on the internet. Software is generally open source or freely downloadable. Protocol specifics are published.	· Bitcoin · Voting system · Ticket selling system
Private	The blockchain is only available on an intranet/VPN. Specifics of the blockchain (genesis block, consensus protocol) are not openly shared	· Invention disclosure database · HR permanent records · Legal compliance records
Permissionless	Anyone who can access the blockchain can submit data to be added to blocks, or can generate and submit blocks to append to the chain	· Bitcoin · Ticket selling system · Invention disclosure database
Permissioned	Parties request access to join, and are admitted or denied. Consensus relies on being able to exclude infractors	· Voting system · HR permanent records · Legal compliance records

Permission and openess?

- Analysis of the use-case determines whether a blockchain should be open/private and permissionless/permissioned

- A further question is whether transaction submission (clients) and block generation and validation (nodes) should be bound by the same rules
  - e.g. an open and permissionless system for submitting a transaction, but open and permissioned for data block validators (so proof-of-work can be avoided)